NCC Operational Systems Rules of Behavior

In accordance with the Office of Management and Budget (OMB) Circular A-130, Appendix III, the following "rules of behavior" are established.

1. Assignment and Limitations of System Privileges: The privileges and quotas provided to you are adequate to perform the normal functions associated with this account.

2. Backup Procedures: The system will be backed-up daily, weekly, and upon installation of new software. Each operator is responsible for backing-up any personal files.

3. Connection to the Internet: Connection to the Internet from the NCCDS (OCR, ANCC, or T&T) is not allowed.

Access to and use of the Internet will only be for official purposes in the conduct of your duties.

Electronic communications facilities (such as e-mail and Netnews are for authorized Government use only.

Email will only be used for official purposes and will not be used to transmit the following information:

a. U. S. Government or corporate credit card numbers
b. Designated Sensitive Data
c. Risk Assessments
d. For Official Use Only information
e. Privacy Act Data
f. Proprietary Data
g. Procurement Sensitive Data
h. Source Evaluation Board (SEB) information

4. Consequences of Behavior Inconsistent with the Rules: Failure to adhere to these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

5. Dial-In Access: Dial-In access to the NCCDS (OCR, ANCC, or T&T) is not allowed.

6. Disposal of IT Resources: Fixed media will be erased prior to transferring the IT resources or designating the resource for excess.

7. Individual Accountability: Center IT resources will not be used or fraudulent, harassing or obscene messages and/or materials.

Tampering with another person's account, files or processes without the other person's express permission, use of the system resources for personal purposes, or other unauthorized activities is strictly prohibited and will result in disciplinary action.

Logon ID's and passwords may never be transferred or shared for any reason.

Active logons should never be left unattended.

Workstations will be paused when unattended for short periods of time (less than 30 minutes).

Do not logon to more than one workstation/terminal unless you can keep each of them under constant surveillance.

Personally owned, provided or downloaded software may not be installed.

Classified information will not be entered into the computer system.

When access is no longer required to these IT resources, notify appropriate responsible parties and make no further attempt to access these resources.

No IT resources will be removed from GSFC without a property pass from the property custodian

8. Limits on System Interconnection: System interconnection is under control of the CCB. Any changes to the system interconnections require an approved Engineering Change (EC) or Engineering Test Notice (ETN).

9. Password Management: Passwords

a. Will be a minimum of 6 alphanumeric characters (preferably 8)
b. Will be changed at least every 180 days, will not be a word appearing in an English or foreign dictionary
c. Will be memorized and not written down
d. Will not be stored in keyboard macros or .bat files
e. Will not consist of personal ID data or be easily "guessable"

10. Proper Use of Copyrighted Software: Licensed software will only be used in accordance with the license.

All software on the computer system is protected in accordance with NASA and Federal Government security and control procedures, which will be adhered to.

11. Reporting of IT Security Incidents: Any unauthorized penetration attempt, unauthorized system use, or virus activity will be reported to your supervisor.

12. Restoration of Service: Restoration of service is the responsibility of the Technical Manager with the support of the Operations Engineer and the System Administrator.

13. Unofficial Use of Government Equipment: The computer system you are operating may only be used for official purposes in the conduct of your duties.

Use of the NCC systems for other than official U. S. Government business is a violation of federal law.

Use of these information technology (IT) resources gives consent for monitoring and security testing to ensure proper security procedures and appropriate usage are being observed for Center IT resources.

14. Work at Home: The CNE Project purchased the Annex to provide GSFC personnel with a means to connect to the Goddard network from home or while on travel. Its intent is to allow GSFC personnel a method of checking e-mail and doing other limited work from home or while on travel. This is a government computer resource, for use by government employees and Approved contractors, and is to be used only for government related work. If it is discovered that resources are being misused, your dial up account will be deleted and further appropriate action may be taken.

15. Facility Considerations: Challenge anyone in the computer facility that does not have an appropriate
Badge.

Rooms with workstations or terminals must be locked after normal working hours except when such workstations or terminals are located in continuously manned Operational areas.